Burdon, Mark and von Nessen, Paul and Reid, Jason F. and Lane, William B. (2010) ***Australian data breach notification : avoiding the State/Federal overlap.*** In: Proceedings of 5th International Conference on Legal, Security and Privacy Issues in IT Law, 3-5 November 2010, Universitat Pompeu Fabra, Barcelona.

Australian Data Breach Notification: Avoiding the State/Federal Overlap

Mark Burdon,[*] Paul von Nessen,[†] Jason Reid[*] and Bill Lane[*]

Mandatory data breach notification has become a matter of increasing concern for law reformers. In Australia, this issue was recently addressed as part of a comprehensive review of privacy law conducted by the Australian Law Reform Commission (ALRC) which recommended a uniform national regime for protecting personal information applicable to both the public and private sectors. As in all federal systems, the distribution of powers between central and state governments poses problems for national consistency. In the authors' view, a uniform approach to mandatory data breach notification has greater merit than a 'jurisdiction specific' approach epitomized by US state-based laws. The US response has given rise to unnecessary overlaps and inefficiencies as demonstrated by a review of different notification triggers and encryption safe harbors. Reviewing the US response, the authors conclude that a uniform approach to data breach notification is inherently more efficient.

1. Introduction

Australia, like the United States, operates on a federal system of government, with powers distributed between the central, Commonwealth government and those of the six states under the Australian Constitution. When the Australian Commonwealth was established in 1901, the framers of the Australian Constitution sought guidance about an appropriate federal system from the United States[1] - more so than from Canada, which might have been considered a more obvious model from the British

[*] Queensland University of Technology, Australia.

[†] Monash University and Consultant, McCullough Robertson Lawyers, Australia. The authors gratefully acknowledge funding from Australian Research Council Grant DP0879015 "A new legal framework for identifying and reporting Australian data breaches."

[1] The effect of the Australian constitutional framers is neatly summarized in *R. v Kirby ex parte The Boilermakers Soc. of Austl. (Boilermakers),* (1956) 94 CLR 254 at 275:

> Probably the most striking achievement of the framers of the Australian instrument of government was the successful combination of the British system of parliamentary government containing an executive responsible to the legislature with American federalism.

Commonwealth.[2] As a consequence, the Australian Constitution includes many provisions modeled on, or adapted from those found in the United States Constitution.[3]

The division of powers under the Australian Constitution, like those in other federated systems, is often explained by historic justifications, based upon geopolitical realities of the eighteenth and nineteenth century. In that respect, developments of the modern era pose challenges not foreseen in past years. This is obvious in relation to phenomena such as the emergence of integrated financial markets and rapid developments in information technology and infrastructure, all of which result in the continuing diffusion of regulatory power. The manner in which federal systems must adapt in response to challenges of this nature is evident, for example, in the field of corporations law, where Australia, after protracted efforts, managed to achieve a uniform legal approach, based on a consensus forged between the federal and state governments. The developing area of information privacy law presents a similar challenge.

Bearing in mind the legislative constraints imposed by a federal system of government, this paper considers the pitfalls involved in a legal response to data breaches which is based on a narrow, 'jurisdiction by jurisdiction' legislative approach. By contrasting US experience with the manner in which the issue is being addressed in Australia, the authors contend that, at least for Australia, one voice rather than many is more likely to provide optimal solutions in relation to mandatory data breach notification.

2. Australian Privacy Regulation Developments

In Australia, mandatory data breach notification has been addressed as a component of privacy law reform. Currently, the federal *Privacy Act 1988 (Cth)* (hereafter "the *Privacy Act*") regulates the handling and use of personal information in those spheres in which the Commonwealth parliament can legislate – principally, the federal public sector (including that of the Australian Capital Territory) and the private sector. In its original form, the Act established a set of Information Privacy Principles (IPPs), modeled on OECD guidelines,[4] to regulate the handling of personal information by those government departments and agencies to which the Act applied. The Office of the Privacy Commissioner was also established to oversee and regulate their implementation. Later, in 1990, the Act was amended to extend these privacy safeguards to an area of the private sector concerned with consumer credit reporting.[5] By further amendment in 2000, the Act was extended to all private sector organizations which were made subject to a set of privacy principles designated as the National Privacy Principles (NPPs).[6]

---

[2] *See* QUICK, AND GARRAN, ANNOTATED CONSTITUTION OF THE AUSTRALIAN COMMONWEALTH (Angus and Robertson, Sydney, 1901).

[3] *See* HUNT, AMERICAN PRECEDENTS IN AUSTRALIAN FEDERATION (Columbia University Press, New York, 1930).

[4] ORG. FOR ECON. CO-OPERATION AND DEV. [OECD], *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at* http://www.oecd.org/document/ 18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html.

[5] PRIVACY AMENDMENT ACT 1990 (Cth) (Austrl.).

[6] PRIVACY AMENDMENT (PRIVATE SECTOR) ACT 2000 (Cth) (Austrl).

However, in 2006, following further concerns expressed about diminishing privacy protection[7] - and consistent with international developments, the then Attorney-General of Australia, the Hon. Philip Ruddock, requested the Australian Law Reform Commission (ALRC) to undertake a review of the federal *Privacy Act* to ascertain whether it continued to provide an effective framework for the protection of privacy in Australia. In terms of its regulation of personal information, the *Privacy Act* does not seek to cover the field - each Australian state and territory also has legislation or administrative guidelines, principally for the regulation of its own public sector. And state-based inquiries similar to that requested of the ALRC have also been, or are being, conducted by the Victorian Law Reform Commission[8] and the New South Wales Law Reform Commission.[9]

Referring to this federal/state overlap of responsibility in Australia, the ALRC pointedly noted:

> This creates confusion for individual consumers, who cannot always be expected to know whether an agency is a federal, state or territory body or, as a result, where to go for guidance on which privacy laws apply or where to take concerns and complaints.

In relation to the *Privacy Act*, the ALRC commenced its inquiry in 2006, provided its initial findings in 2007,[10] and in May, 2008 gave its final recommendations in Report 108, *For Your Information: Australian Privacy and Practice.*[11] The ALRC's recommendations are extensive. Many propose modernizing and harmonizing the privacy obligations already applicable in their previous form to private and public sector organizations. One major recommendation, for example, concerns the introduction into the Australian privacy legislation of the Uniform Privacy Principles applicable to governmental agencies and private organizations alike.[12] These new principles would deal with collection of personal information,[13] notification that the collection has

---

[7] AUSTRALIAN LAW REFORM COMMISSION, Review of Privacy: Issues Paper (Australian Law Reform Commission. 2007).

[8] VICTORIAN LAW REFORM COMMISSION, WORKPLACE PRIVACY: FINAL REPORT (2005).

[9] NEW SOUTH WALES LAW REFORM COMMISSION, CONSULTATION PAPER 1, INVASION OF PRIVACY (NSWLRC CP 1). The final report is expected soon.

[10] AUSTRALIAN LAW REFORM COMMISSION, Review of Australian Privacy Law (Australian Law Reform Commission. 2007).

[11] AUSTRALIAN LAW REFORM COMMISSION, FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE (Australian Law Reform Commission. 2008) hereafter [PRIVACY LAW AND PRACTICE].

[12] AUSTRALIAN LAW REFORM COMMISSION, Review of Privacy: Issues Paper, 34. Recommendation 18–2 states:

> The *Privacy Act* should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles, referred to in this Report as the model Unified Privacy Principles.

[13] *Id.* at 91-2. The proposed Uniform Privacy Principles (UPP) in relevant part provides:

> 2.1 An agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.
>
> 2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
>
> 2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

occurred,[14] the permissible use of such information,[15] and the accuracy[16] of such information.

As a result of the overlap of Commonwealth and State legislation, the ALRC also indicated that this continuing problem should be addressed. In its view, there would be great benefits across the board from adopting a common approach to privacy protection in all Australian jurisdictions. To achieve greater consistency, the ALRC recommended that the *Privacy Act* should apply to the federal public sector and the private sector to the exclusion of state and territory laws covering such matters. Further, the ALRC recommended that the Commonwealth, state and territory governments establish an intergovernmental cooperative scheme, under which the states and territories would enact legislation to regulate the handling of personal information in each state's and territory's public sector by adopting the key elements of the *Privacy Act*—such as the same set of privacy principles, important definitions, data breach notification schemes and other key provisions.

The Australian model of one uniform approach to privacy legislation is similar to that used to bring in uniform corporate and securities laws from 1990 (ultimately resulting in complete federalization of that area of law). The disadvantages of multiple approaches to privacy regulation can be seen in the United States, where both the Federal government and the various states have dealt with the concept of data breach notification. In consequence of this dispersal of responsibility, both the exemption for encryption of data from the data breach statutes and the notification requirements under

---

2.4 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:

(a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or

(b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

2.5 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

(a) the individual has consented…

[14] *Id* at 93. Uniform Privacy Principle 3, Notification, provides that when an agency or organisation collects personal information about an individual, it should take reasonable steps to notify the individual of the collection of the information, the purposes of its collection and the types of organisation to whom such information is likely to be disclosed. It also provides for access and correction (further dealt with in Uniform Privacy Principle 9) as well as complaint mechanisms.

[15] *Id*. at 94. Uniform Privacy Principle 5, Use and Disclosure, indicates that an agency or organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection with certain exceptions. These exceptions include related secondary purposes which would be reasonably expected, those for which the individual has consented, disclosures to protect the individual life, health or safety or the public health or safety, and, under prescribed circumstances, to enforcement agencies.

[16] *Id.* at 97. Uniform Privacy Principle 7, Data Quality, states that an agency or organisation must take reasonable steps to make certain that the personal information it collects, uses or discloses is accurate, complete, up-to-date and relevant.

the various statutes indicate a complexity and inefficiency which the Australian proposal (nascent though it is) may avoid these complexities if the ALRC's recommendation on intergovernmental cooperation is adopted.

3. Data Security and Data Breach Notification – the Uniform Australian Approach

Among the most significant of the recommendations concerning privacy in the ALRC report are those relating to the security of data and the obligations which arise where that security has been compromised. The proposed Uniform Privacy Principles continue the obligation on data holders to maintain security over the personal information they hold,[17] indicating that:

> An agency or organization must take reasonable steps to: protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.[18]

Concern was also expressed for the need for a protocol when the security of data had been breached. In early 2008, concurrent with the ALRC inquiry into the state of the *Privacy Act*, the Office of the Privacy Commissioner released a consultation paper on a Voluntary Information Security Breach Notification Guide to enable organizations and agencies to respond effectively to an information security breach.[19] While the voluntary guidelines could operate immediately for those willing to adopt them, the Privacy Commissioner also supported the inclusion of provisions to the *Privacy Act* that would require organizations to advise affected individuals of the breach of their personal information in certain circumstances.[20] The ALRC clearly took on board the suggestions of the Privacy Commissioner, devoting a whole section of its final report to data breach notification and the benefits of the various legislative models.[21] Moreover, the ALRC confirmed its discussion paper proposals, recommending that the *Privacy Act* be amended to include a new part on data breach notification. The proposal reads as follows:[22]

> **Recommendation 51–1** The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows:
> (a) An agency or organization is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorized person and

---

[17] PRIVACY ACT 1988 (CTH) (Austrl.) S 14, IPP 4; SCH 3, NPP 4.

[18] AUSTRALIAN PRIVACY LAW AND PRACTICE, *supra* note 11, at 98. Uniform Privacy Principle 8.1(a). Part (b) provides:

> An agency or organisation must take reasonable steps to: (b) destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law.

[19] AUSTRALIAN GOVERNMENT OFFICE OF THE FEDERAL PRIVACY COMMISSIONER CONSULTATION PAPER—DRAFT VOLUNTARY INFORMATION SECURITY BREACH NOTIFICATION GUIDE (2008).

[20] Id. at 18 (stating that the voluntary guidelines are not intended to be a substitute for further legislative action, but are aimed at encouraging voluntary action to address these issues while legislative change is under consideration).

[21] AUSTRALIAN PRIVACY LAW AND PRACTICE, *supra* note 11, at 1696.

[22] *Id* at 1696-7.

the agency, organization or Privacy Commissioner believes that the unauthorized acquisition may give rise to a real risk of serious harm to any affected individual.

(b) The definition of 'specified personal information' should include both personal information and sensitive personal information, such as information that combines a person's name and address with a unique identifier, such as a Medicare or account number.

(c) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:

(i) whether the personal information was encrypted adequately; and

(ii) whether the personal information was acquired in good faith by an employee or agent of the agency or organization where the agency or organization was otherwise acting for a purpose permitted by the *Privacy Act* (provided that the personal information is not used or subject to further unauthorized disclosure).

(d) An agency or organization is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.

(e) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.

While the data breach statute is likely to evolve as a result of international experience, it is probable that one data breach statute, whatever its eventual form, will apply throughout Australia. This would make it far easier for individuals to understand the general rules that apply to personal information regardless of whether it is being handled by a private organization, a federal agency, or a state or territory agency. In contrast to the way the United States requirements have evolved, discussed below, a uniform and cooperative data breach notification statute enacted in similar terms by the Commonwealth government and the States would ease the compliance burden significantly and reduce costs for business.

4. US State Law Notification Triggers & Encryption Safe Harbors

The difficulties that arise from state/federal overlaps in data breach notification become readily visible upon an examination of the development of state-based notification triggers and encryption exemptions which demonstrate the plethora of statutory constructions in existence.

4.1 Notification Triggers

A key difference and point of contention between US state-based data breach notification laws regards notification triggers. The notification trigger is the statutory requirement that indicates when and in what circumstance notification is required from an organization. A majority of state-based laws are largely based on the Californian model[23] but some state laws have adopted different types of notification trigger that can

[23] *See* Sean C Honeywill, *Data Security and Data Breach Notification for Financial Institutions*, 10 NORTH CAROLINA BANKING INSTITUTE 269(2006).

be broadly categorized into two types: acquisition based and risk-based triggers that represent differing approaches to notification.[24]

Acquisition based triggers, such as the California law, have a relatively low 'triggering threshold' that triggers an obligation to notify when an organization has suffered, or believes it has suffered a breach.[25] Accordingly, notification may be required even when there is no actual evidence of data having been acquired.[26] Jones contends that data breach notification laws based on an acquisition trigger are more consumer oriented because broad notification means that consumers are made aware of potential data breaches and can therefore take action to mitigate potential harms before they arise.[27] Acquisition-based triggers therefore set a minimum threshold for notification in relation to identity theft risks.[28] Risk-based triggers, on the other hand, set a different standard as these triggers only require notification in situations where a risk assessment determines that a risk of harm exists to consumers.[29] Jones contends that risk-based triggers are business oriented because they generally require the corporate entity to make a determination whether a risk of harm will or is reasonably likely to arise.[30]

The distinction between an acquisition-based trigger and a risk-based trigger goes to the heart of data breach notification's rationale and it also signifies some major differences between different approaches. Acquisition-based triggers employ the regulatory tool of reputational sanction.[31] Notification is used as a threat held over the

---

[24] *See* Michael E Jones, *Data Breaches: Recent Developments in the Public and Private Sectors*, 3 I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY 555, 562 (2007). *See also* Martin G Bingisser, *Data Privacy and Breach Reporting: Compliance with Varying State Laws*, 4 SHIDLER JOURNAL OF LAW, COMMERCE & TECHNOLOGY (2008) (defining the distinction as "strict vs. flexible"); Prischia M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECHNOLOGY LAW JOURNAL 1103, 1118 (2009) (ascertaining that trigger choice has also been a political choice).

[25] *See* Jones, surpa note 24, at 562 (regarding the elements of acquisition based triggers that are deemed to favor consumer protection because notification is not left to the breached entity); Paul M Schwartz & Edward J Janger, *Notification of Data Security Breaches*, 105 MICHIGAN LAW REVIEW 913, 933 (2007) (commenting the Californian law "is marked by a low threshold for notification").

[26] Jones, surpa note 24, at 562.

[27] *Id*. at 563.

[28] *See* Samuel Lee, *Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs*, 1 ENTREPRENEURIAL BUSINESS LAW JOURNAL 125, 132 (2006).

[29] *See* FRED H. CATE, *Information Security Breaches: Looking Back and Thinking Ahead*(2008), at http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf., 13; MICHAEL TURNER, *Towards a Rational Personal Data Breach Notification Regime*, *14* (2006), at http://www.infopolicy.org/files/downloads/data_breach.pdf.

[30] Jones, surpa note 24, at 563.

[31] *See* Schwartz & Janger, supra note 25, at 947 (regarding the role and failure of reputational sanction); Jane Winn, *Are 'Better' Security Breach Notification Laws Possible?*, 24 BERKELEY TECHNOLOGY LAW JOURNAL 1133, 1143 (2009) (the shaming function of data breach notification is "direct and concrete").

head of organizations to improve information security measures or else suffer the embarrassment and humiliation of public notification.[32] Notification therefore fulfils both an *ex ante* purpose, through the encouragement of adequate information security practices to minimize data breaches before they arise,[33] and an *ex post* purpose to provide consumers with information in order that they can take action to mitigate themselves.[34] The rationale of acquisition-based notification thus makes in-built judgments about corporate failures to secure personal information and the effectiveness of notification as a remedy.[35]

For the purposes of this article, our interest briefly focuses on the different standards that exist as to what triggers notification under a risk-based trigger as this lays the foundation for a deeper analysis of encryption safe harbors. For example, some US state-based data breach notification laws require a reasonable likelihood that harm may arise[36] where others require a significant or material real risk of identity theft[37] or a reasonable likelihood of substantial economic loss.[38] Some risk-based triggers therefore operate on higher standards for notification than others which complicate compliance requirements for nationwide companies. This point is magnified further by an examination of US state-based encryption safe harbors which moves concerns from compliance complications to the general effectiveness of statutory constructions in relation to data breach notification.

---

[32] *See* Schwartz & Janger, supra note 25, at 936-937 (regarding the essential role of reputational sanction in acquisition-based trigger laws). *See also* James T Graves, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WILLIAM MITCHELL LAW REVIEW 1115, 1120 (2008) (contesting that data breach notification law does not adequately deal with corporate information security measures); Jacob W Schneider, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 BOSTON UNIVERSITY JOURNAL OF SCIENCE & TECHNOLOGY LAW 279, 285 (2009) (claiming the reputational detriment has little, long-term practical impact upon corporations).

[33] *See* Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECHNOLOGY LAW JOURNAL 1061(2009) (regarding the ex ante role of security protections to reduce the numbers of future data breaches).

[34] *See Id*. at 1072-1074 (regarding an overview of information disclosure measures as an *ex post* mechanism in data breach notification laws); *See also* Graves, *supra* note 32, at 1122 (questioning the effectiveness of the ex ante elements).

[35] *See* Jonathan J Darrow & Stephen J Lichtenstein "*Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY 1, 50 (2008) (in relation to the time and cost of repairing data breach damage).

[36] *See e.g*. ARK. CODE ANN. § 4-110-105 (Michie 2005); FLA. STAT. § 817.5681 (2005); LA. REV. STAT. ANN. §§ 51:3071 (West 2005).

[37] *See e.g*. KAN. STAT. ANN. §§ 50-7a01 (2006); MD. CODE ANN. §§ 14-3501 (2008); MASS. GEN. LAWS 93H §1 (2007); MICH. COMP. LAWS § 445.72 (2007); OHIO REV. CODE ANN. § 1349.19 (West 2005); R.I. GEN. LAWS § 11-49.2-1 (2005); UTAH CODE ANN. §§ 13-42-101 (2006); WIS. STAT. § 895.507 (2006).

[38] *See e.g.* ARIZ. REV. STAT. § 44-7501 (2007).

4.2 Encryption Safe Harbors

The use of an encryption safe harbor has been an integral element of data breach notification laws because encryption has been used by legislators to define notification parameters for organizations. Put simply, as applied in most data breach notification laws, encrypted personal information does not trigger an obligation to notify because the information that has been acquired without authorization is secure and therefore does not pose an identity theft risk. Jones has identified three types of encryption safe harbor.[39] *Exemptions* exempt notification based on the notion that encrypted data is secure and does not pose a risk. *Rebuttable presumptions* create a presumption that encrypted data is secure and unauthorized acquisitions do not have to be notified. However, this presumption can be rebutted by facts to the contrary. *Factor-based analysis* requires breached organizations to demonstrate that the encryption adopted was effective before notification is exempted. Our research indicates that all but two US state-based laws have exemption type encryption safe harbors.[40]

We identified five conceptual and operational layers that we used to categorize 19 key statutory terms that are currently being used in state-based encryption exemptions. Table 1, below, outlines the layers, statutory terms and their identifiers (e.g. letters A to S). The layers are conceptual and operational categorizations of different security related requirements that classify statutory terms into broad themes that permeate throughout state-based encryption exemptions. The terms are representative of an array of definitions that are essentially used to define different exemption elements and the range of different definitions is highlighted in brackets in the Key Statutory Terms column.

Table 1. Conceptual/Operational Layers and Key Statutory Terms

Layer	ID	Key Statutory Terms (alternate definitions in brackets)
[1] Californian Model	**A**	Requirements of Cal Civil Code 1729(a): unencrypted personal information (personal information is not encrypted; Not secured by encryption).
[2] Encryption Definitions	**B**	Encryption is an algorithmic process that transforms data, unreadable or unusable without confidential process or key.
	C	Encryption is an algorithmic process that transforms data where there is a low probability of assigning meaning without a confidential process or key.
	D	Encryption is the transformation of data using 128 bits or higher: low probability of meaning without confidential process or key.
	E	Encryption is the disguising of data using generally accepted practices.
	F	Data protected by another method to make it unreadable or unusable (Any method secures data: unreadable or unusable; Protected by any method: unreadable or unusable; Secured by another method that renders data unreadable or unusable; Securing by another method; rendering completely unreadable or unusable; Data protected by other methods that make data: unreadable or

[39] Jones, *supra* note 24.

[40] Exceptions being D.C. CODE ANN. § 28-3851 (2007); WYO. STAT. ANN. §§ 40-12-501 (Michie 2007).

Layer	ID	Key Statutory Terms (alternate definitions in brackets)
[3] Other Methods		unusable).
	G	Data transformed by another method or technology to make unreadable or unusable (Any method or technology alters data to make unreadable or unusable).
	H	Data transformed by another method of technology that makes electronic data unreadable or unusable.
	I	Data altered by any method or technology to make it unreadable (Altered in a manner that renders data unreadable).
	J	Data is not rendered unusable through other methods that compromise the security, confidentiality or integrity the data (Data elements are not rendered unusable).
[4] Redaction	**K**	Redacted is undefined.
	L	Redaction is defined as to render or truncate specified forms of numerical data to make unreadable.
	M	Redaction is defined as to alter or truncate specified forms of numerical data to make unreadable.
[5] Key Management	**N**	Data is encrypted and the encryption key was acquired.
	O	Data is encrypted and encryption key was accessed or acquired.
	P	Data is secured and encryption key or password or other means necessary for reading or using the data was acquired.
	Q	Data is not considered encrypted if it is acquired in combination with any required key, security code, access code or password that would permit access.
	R	Encrypted electronic data is acquired or used and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information.
	S	Security breach involves person with access to encryption key.

US state-based encryption exemptions adopt one of two core definitional approaches. The first is whether the state legislation attempts to explicitly define encryption or whether the exemption is of a non-explicit variety as based on the Californian law. Layer 1, Californian Model represents the latter and Layer 2, Encryption Definitions detail different attempts to define encryption. The complexity of different definitions varies from the straightforward[41] to the technically specific.[42] Within Layer 2, there is a majority definition of encryption in operation[43] but encrypted

[41] *See e.g.* ME. REV. STAT. ANN. 10, §§ 210-B-1346 (West 2007) ("encryption is the disguising of data using generally accepted practices").

[42] *See e.g.* MASS. GEN. LAWS 93H §1 (2007) ("encryption is the transformation of data using 128 bits or higher to which encrypted data has a low probability of meaning without access to a confidential process or key").

[43] The basis of the majority definition is "encryption is an algorithmic process that transforms data."

data is defined in two ways: (1) data that is unreadable or unusable[44] or (2) data that has a low probability of meaning without access to a confidential process or key.[45] Layer 3, Other Methods, details statutory terminology that is often adopted in state-based laws which provides for the use of methods[46] or methods and technologies[47] or technologies only,[48] in addition to encryption, that renders data unreadable or unusable. There are also variations that entail differences between data that is unreadable only[49] and unusable only.[50] However, these laws generally provide no indication as to what methods or technologies would equate to encryption. Layer 4, Redaction, highlights those states that have extended their encryption exemption to also cover redaction. Again, as above, there is a difference between those states that attempt to define redaction[51] and those that do not.[52] Finally, Layer 5, Key Management, details those states that also require some form of security in relation to decryption keys, passwords or other codes that would enable an

---

[44] *See* MASS. GEN. LAWS 93H §1 (2007); ARI REV. STAT. § 44-7501 (2007); HAW. REV. STAT §§ 487N-1 (2007); IOWA CODE § 715C.1 (2008); MO. REV. STAT. § 407.1500 (2009); NEB. REV. STAT. §§ 87-801 (2006); N.C. GEN. STAT. §§ 75-60 (2005); 9 VT. STAT. ANN. §§ 2430 (2007).

[45] *See* MD. CODE ANN. §§ 14-3501 (2008); MICH. COMP. LAWS § 445.72 (2007); OHIO REV. CODE ANN. § 1349.19 (West 2005); N.H. REV. STAT. ANN. §§ 359-C:19 (2007); VA. CODE ANN. § 18.2-186.6 (Michie 2008); W. VA. CODE §§ 46A-2A-101 (2008).

[46] *See* KAN. STAT. ANN. §§ 50-7a01 (2006); MD. CODE ANN. §§ 14-3501 (2008); MICH. COMP. LAWS § 445.72 (2007); UTAH CODE ANN. §§ 13-42-101 (2006); ARIZ. REV. STAT. § 44-7501 (2007); MO. REV. STAT. § 407.1500 (2009); 9 VT. STAT. ANN. §§ 2430 (2007); VA. CODE ANN. § 18.2-186.6 (Michie 2008); W. VA. CODE §§ 46A-2A-101 (2008); COLO. REV. STAT. § 6-1-716 (2006) (2006); IND. CODE §§ 24-4.9-3-1 (2006).

[47] *See* CONN. GEN. STAT. § 36a-701b (2006); N.J. STAT. ANN. § 56:8-163 (West 2006); N.D. CENT. CODE §§ 51-30-01 (2005).

[48] *See* MINN. STAT. § 325E.61 (2006).

[49] *See* OHIO REV. CODE ANN. § 1349.19 (West 2005); WIS. STAT. § 895.507 (2006); IOWA CODE § 715C.1 (2008); NEB. REV. STAT. §§ 87-801 (2006); ALASKA STAT. § 45.48.010 (Michie 2009).

[50] *See* OR. REV. STAT. § 646A.600 (2007); S.C. CODE ANN. § 39-1-90 (Law Co-op 2009).

[51] *See* KAN. STAT. ANN. §§ 50-7a01 (2006); MICH. COMP. LAWS § 445.72 (2007); OHIO REV. CODE ANN. § 1349.19 (West 2005); ARIZ. REV. STAT. § 44-7501 (2007); IOWA CODE § 715C.1 (2008); MO. REV. STAT. § 407.1500 (2009); NEB. REV. STAT. §§ 87-801 (2006); N.C. GEN. STAT. §§ 75-60 (2005); 9 VT. STAT. ANN. §§ 2430 (2007); VA. CODE ANN. § 18.2-186.6 (Michie 2008); W. VA. CODE §§ 46A-2A-101 (2008); IND. CODE §§ 24-4.9-3-1 (2006); ALASKA STAT. § 45.48.010 (Michie 2009).

[52] *See* ARK. CODE ANN. § 4-110-105 (Michie 2005); LA. REV. STAT. ANN. §§ 51:3071 (West 2005); MD. CODE ANN. §§ 14-3501 (2008); WIS. STAT. § 895.507 (2006); ME. REV. STAT. ANN. 10, §§ 210-B-1346 (West 2007); COLO. REV. STAT. § 6-1-716 (2006); OR. REV. STAT. § 646A.600 (2007); S.C. CODE ANN. § 39-1-90 (Law Co-op 2009); GA. CODE ANN. §§ 10-1-911 (2005); 815 ILL. COMP. STAT. 530/1 (2005).

unauthorized person to decrypt acquired personal data.[53] One state also includes the situation where a person who had access to decryption keys was also involved in the breach.[54]

As highlighted above, a layering process starts from a foundational layer.[55] There are four groups of encryption exemption that start with the Californian law, beginning with Term A and the broad-ranging exemption featuring "unencrypted personal information". In 2005, the next two states to enact data breach laws, North Dakota and Georgia, followed the Californian law but added another layer to the exemption based on the other methods (A,G)[56] and the redaction (A,K)[57] layers respectively. The Georgia exemption was subsequently copied by Arkansas[58] in August 2005 and Illinois[59] and Louisiana[60] in January 2006. In December 2005, the New York law was then enacted and added a term from the key management layer to its definition of personal information (A,N).[61] Minnesota is then the first Californian based exemption to include terms from all three layers which are different to those previously adopted (A,H,P).[62]

The second layering effect then starts to become more apparent. In early 2006, for the first time, we have several states that layer an additional term over another additional term. For example, the Colorado law[63] adds a term from the other methods layer to a pre-existing redaction layer (A,F,K) as does the Wisconsin law (A,I,K).[64] This process then continues throughout the incorporation of the Californian law until the most recent laws to be enacted in Alaska (A,J,K)[65] and South Carolina (A,I,M).[66] In January 2007, the Utah law also adds Colorado's term from the other methods layer but does not incorporate the redaction term - a different element from the other methods layer (A,F).[67] The Californian based exemptions use a wide range of terms from different layers but only repeat certain terms infrequently, particularly term K.

---

[53] *See* MASS. GEN. LAWS 93H §1 (2007); N.C. GEN. STAT. §§ 75-60 (2005); N.H. REV. STAT. ANN. §§ 359-C:19 (2007); MINN. STAT. § 325E.61 (2006); OR. REV. STAT. § 646A.600 (2007).

[54] *See* 73 PA. CONS. STAT. § 2303 (2006).

[55] It should also be noted that some states simply adopted the Californian notification trigger word for word and they therefore have identical encryption exemptions. Those state laws are: FLA. STAT. § 817.5681 (2005); R.I. GEN. LAWS § 11-49.2-1 (2005); 6 DEL. CODE ANN. §§ 12B-101 (2005); IDAHO CODE § 28-51-104 (Michie 2006); MONT. CODE ANN. § 30-14-1704 (2006); NEV. REV. STAT. §§ 603A.010 (2006); OKLA. STAT. § 74-3113.1 (2006); TENN. CODE ANN. § 47-18-2101 (2005); TEX. BUS. & COMM. CODE. §§ 48.001 (2005); WASH. REV. CODE § 19.255.010 (2005).

[56] N.D. CENT. CODE §§ 51-30-01 (2005).

[57] GA. CODE ANN. §§ 10-1-911 (2005).

[58] ARK. CODE ANN. § 4-110-105 (Michie 2005).

[59] 815 ILL. COMP. STAT. 530/1 (2005).

[60] LA. REV. STAT. ANN. §§ 51:3071 (West 2005).

[61] N.J. STAT. ANN. § 56:8-163 (West 2006).

[62] MINN. STAT. § 325E.61 (2006).

[63] COLO. REV. STAT. § 6-1-716 (2006).

[64] WIS. STAT. § 895.507 (2006).

[65] ALASKA STAT. § 45.48.010 (Michie 2009).

[66] S.C. CODE ANN. § 39-1-90 (Law Co-op 2009).

[67] UTAH CODE ANN. §§ 13-42-101 (2006).

The same type of foundational and supplementary layering is evident amongst those states that have attempted to define encryption. However, it is more common for certain terms to be copied and used with different terms from the same layer. This promotes a clustering effect where different states adopt clusters of the same set of terms. The foundational base of the majority of these states represents the difference between terms B and C, and a choice based on either the North Carolinian[68] or the Ohio law[69]. The North Carolina law appeared relatively early in the development of encryption exemptions following enactment in December 2005. The law was also enacted with terms from the redaction and key management layers (B,L,O). In March 2006, the Nebraska law used Term B as the basis for its exemption but then added different terms from the other methods and redaction layers (B,I,M). Vermont (B,F,L)[70] and Arizona (B,F,M)[71] then follow suit in January 2007 but again use a combination of different terms. The clustering effect then becomes visible as the North Carolina exemption was followed by Hawaii (B,L,O);[72] Iowa(B,I,M)[73] follows Nebraska and in 2009 Missouri (B,F,M)[74] follows Arizona. Separate from the other Term B states is Oregon which is the only exemption that includes terms from all three additional layers (B,J,K,N) which have been adopted from the Californian based exemptions.[75]

A similar effect is also identifiable in the development of the Term C states. Those states that have adopted Term C as their foundational base began with Ohio in February 2006 which also implemented terms from the redaction and other methods layers at the onset of enactment (C,I,M). The Ohio law also adopted a different definition of redaction to the Californian based exemptions and Term B based states (M).[76] Pennsylvania[77] then adopts the same definition of redaction but also includes a term from the key management later (C,M,S). Indiana[78] then founds the most popular exemption amongst the Term C states that involves terms from the other methods and redaction layers (C,F,M) and is subsequently adopted by four other states.[79] Finally, New Hampshire[80] uses Term F with a key management term (C,F,Q) and Maryland[81] uses Term F with a different redaction term (C,F,K).

5. The US Approach – Many Hands

We contend that the layering effect has had a detrimental effect regarding the coherent development of US state-based encryption exemptions. For example, different foundational layers set higher and lower standards as to what constitutes encryption.

---

[68] N.C. GEN. STAT. §§ 75-60 (2005).
[69] OHIO REV. CODE ANN. § 1349.19 (West 2005).
[70] 9 VT. STAT. ANN. §§ 2430 (2007).
[71] ARIZ. REV. STAT. § 44-7501 (2007).
[72] HAW. REV. STAT §§ 487N-1 (2007).
[73] IOWA CODE § 715C.1 (2008).
[74] MO. REV. STAT. § 407.1500 (2009).
[75] OR. REV. STAT. § 646A.600 (2007).
[76] OHIO REV. CODE ANN. § 1349.19 (West 2005).
[77] 73 PA. CONS. STAT. § 2303 (2006).
[78] IND. CODE §§ 24-4.9-3-1 (2006).
[79] *See* KAN. STAT. ANN. §§ 50-7a01 (2006); MICH. COMP. LAWS § 445.72 (2007); VA. CODE ANN. § 18.2-186.6 (Michie 2008); W. VA. CODE §§ 46A-2A-101 (2008).
[80] N.H. REV. STAT. ANN. §§ 359-C:19 (2007).
[81] MD. CODE ANN. §§ 14-3501 (2008).

Those laws based on Term C state that encryption is an algorithmic process that transforms data where there is a *low probability* of assigning meaning without a confidential process or key. However, Term B uses the same terminology except that it has a higher standard namely, encrypted data is *unreadable or unusable* without access to a confidential process or key. The use of the phrase 'low probability' is different from 'unreadable or unusable' because it is not an absolute (i.e. the data is either readable or usable or it is not). The use of low probability therefore connotes that encrypted data is never believed to be absolutely secure. Potential problems can arise for those laws that combine both elements such as when some of the Term C states use terms from the other methods layer based on unreadable or unusable.[82] These laws effectively have two different operational standards with the other methods exemption operating at a higher level than the encryption exemption. The same applies to those Term B states, Nebraska and Iowa that have adopted North Carolina's definition of encryption but have also adopted Ohio's other methods term.[83]

We also identify a concern that arises with the use of Ohio's other methods term (I). Ohio adopts a different other methods term from those states that subsequently adopted the law's Term C foundation. Data can be considered for a safe harbor if it has been altered by a method or technology that makes it unreadable.[84] The use of a hash function is an important consideration in this regard. While it violates accepted best practice, a hash function is sometimes used to transform credit card numbers in a way that makes them unreadable. It could therefore potentially be considered as an appropriate method or technology for reliance upon a safe harbor. However, just because the hashed data is unreadable, it does not mean to say that it is unusable.[85] With some additional analysis, unreadable data can still reveal useful information. The use of an exclusory term based on *unreadable* therefore sets a lower standard than is implied *by unusable*.

The combination of encryption and redaction can also be problematic particularly for laws that do not attempt to define redaction. In its strict legal sense, the process of redaction refers to blacking out of words in hard copy documents to restrict the publication of sensitive information.[86] The electronic equivalent of hard copy redaction is difficult to achieve as has been demonstrated in recent high-profile reported

---

[82] *See* KAN. STAT. ANN. §§ 50-7a01 (2006); MD. CODE ANN. §§ 14-3501 (2008); MICH. COMP. LAWS § 445.72 (2007); N.H. REV. STAT. ANN. §§ 359-C:19 (2007); IND. CODE §§ 24-4.9-3-1 (2006).

[83] *See e.g.* NEB. REV. STAT. §§ 87-801 (2006) and compare the definition of encryption at §87-802(3).

[84] OHIO REV. CODE ANN. § 1349.19 (West 2005).

[85] The data is still useable because if the same data is hashed it will produce the same output hash value. Hashed data is therefore susceptible to so called 'dictionary attacks'. It the case of credit card numbers, a dictionary attack involves sequentially hashing all possible credit card numbers - any matches to the stored values reveals a valid credit card number. This is possible because a hash function does not require a secret key as an input to the function.

[86] *See e.g.* BRYAN A. GARNER & HENRY CAMPBELL BLACK, BLACK'S LAW DICTIONARY (West 9th ed. ed. 2009). Redaction is defined as "The careful editing of a document, especially to remove confidential references or offensive material."

examples.[87] Thus the application of redaction elements to electronic data is fraught with problems. Electronic data can be deleted but there is no non-reversible digital analogue of a black marker pen if the text remains present in the electronic file.[88] Redaction therefore is presumably meant to take its lay definition which is "the action or process of revising or editing text especially in preparation for publication."[89] Support for this proposition can be found in state laws that have defined redaction as a process to render (or alter) or truncate data to make unreadable.[90] However, whichever meaning is meant to be applied, a major problem nonetheless arises from the combination of redaction and encryption in an exemption because redaction is given the same weight as encryption when in many cases it should not be because it is trivially reversible. Guidance produced by the US Government's Department of Health and Human Services in relation to security rules for the Health Information Portability and Accountability Act (HIPAA) make it clear that redaction should not be considered as secure as encryption and should only be used with paper records.[91] Accordingly, the lower standard that redaction sets nullifies the higher standards offered by properly implemented encryption when combined together.

These differences highlight an ongoing debate that is currently taking place within the US data breach notification literature. One of the general criticisms of data breach notification laws, particularly US state-based laws is the extraordinary collection of statutory constructions in operation. For example, Picanso, whilst calling for the development of a uniform federal data breach law, highlights the compliance difficulties that have arisen for nationwide businesses due to use of different statutory language by state legislatures.[92] However, as Picanso further points out, federal proposals have not been immune from this criticism either.[93] Rode contests, with reference to the

---

[87] *See* JAIKUMAR VIJAYAN, *TSA Posts Document on Airport Screening Procedures Online - Lawmakers Call Gaffe Shocking, Demand Invesitgation*, Computerworld Security,(2009), at http://www.computerworld.com/s/article/9141982/TSA_posts_document_on_airport_screening_procedures_online. For example, the US Transport Security Administration published a highly sensitive document on the web that was supposedly redacted by drawing black boxes over the relevant text. However "PDF documents don't really care about the black box … and the actual content of the document is still in the file."

[88] This is the case notwithstanding that it may not be displayed on screen or in printed versions of the document. However, if an electronic document is simply a scanned version of paper document that has been physically altered so that the redacted text is no longer visible, the redaction will be effective.

[89] The Oxford English Dictionary definition of redaction.

[90] *See e.g.* KAN. STAT. ANN. §§ 50-7a01 (2006); MICH. COMP. LAWS § 445.72 (2007); OHIO REV. CODE ANN. § 1349.19 (West 2005); ARIZ. REV. STAT. § 44-7501 (2007); WYO. STAT. ANN. §§ 40-12-501 (Michie 2007); IOWA CODE § 715C.1 (2008); MO. REV. STAT. § 407.1500 (2009); NEB. REV. STAT. §§ 87-801 (2006); 9 VT. STAT. ANN. §§ 2430 (2007); IND. CODE §§ 24-4.9-3-1 (2006).

[91] DEPARTMENT OF HEALTH AND HUMAN SERVICES, 45 CFR PARTS 160 AND 164 - BREACH NOTIFICATION FOR UNSECURED PROTECTED HEALTH INFORMATION. (2009), 42742

[92] Kathryn E Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM LAW REVIEW 355, 382 (2006).

[93] *Id*. at 382.

Californian law, that the use of vague language will ultimately render the law useless in the face of continuing technological advances.[94] This criticism does not just apply to the Californian law but a majority of state-based laws that are also based on the Californian definition of personal information. The use of vague language also creates a tendency toward over-regulation because a breached entity is likely to be overly cautious in terms of who gets notified due to legal uncertainty and the technical difficulties in ascertaining those individuals that may have been affected by the breach.[95] Faulkner also contends that the lack of uniform definitions for the key elements of data breach notification[96] is another major problem of US state-based laws. This problem is exacerbated because data breach notification laws are still in their infancy and have yet to be tested through the development of jurisprudential discourse.[97]

However, other authors assert that the development of the state-based laws has many positive attributes. For example, Schwartz contends that the state-based data breach notification laws were the first to recognize an area of regulatory significance whilst federal proposals have remained relatively inert.[98] Similarly, Garcia states that the laws are in effect an "experiment to generate new ideas, testing the range of state laws against the ongoing breaches" and differences should therefore be encouraged.[99] As regards the use of different statutory language, Needles asserts that the development of state-based laws has permitted the inclusion of additional data protection measures through a process of layering.[100] Thus states "have begun to layer affirmative data protection obligations over notification laws, requiring businesses in their jurisdictions to provide security measures for personally identifiable information."[101] This increases the states' "current ability to layer proactive, protective measures over reactive, retributive measures [which] further enhances legislatures' power to craft law to best suit states' needs."[102] This layering process therefore entails the overlaying of additional security measures over a core foundational centre which means that states can tailor their data

---

[94] Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 HOUSTON LAW REVIEW 1597, 1622 (2007).

[95] *Id.*

[96] For example, the concept of personal information in data breach notification laws refers to a combination of name in conjunction with other potentially personally identifying information. *See e.g.* CAL. CIV. CODE §.1789.29(e) (West 2003). Different states have used a combination of many different types of information. *See e.g.* Sara A. Needles, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 North Carolina Law Review 267, 275 (2009).

[97] Brandon Faulkner, *Hacking into Data Breach Notification Laws*, 59 FLORIDA LAW REVIEW 1097, 1108 (2007).

[98] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE LAW JOURNAL 902, 917 (2009).

[99] Flora J Garcia, *'Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time'* (2007) 17(3) FORDHAM INTELLECTUAL PROPERTY, MEDIA & ENTERTAINMENT LAW JOURNAL 693, 726.

[100] Needles. *supra* note 96, at 291.

[101] *Id.* at 292.

[102] *Id*. at 291.

breach notification laws to align with their expectations regarding data protection and consumer protection measures.[103]

Our research findings highlight that the process of layering has been adopted extensively in the development of state-based exemptions. The use of conflicting statutory terminology is a problem that has been exacerbated by seemingly ad hoc development. The state-based laws were developed in a relatively short period of time and little emphasis seems to have been placed on testing or monitoring the effects of the laws. The result of has been the creation of a plethora of encryption exemptions. A 'pick and mix' mentality to legislative development is prevalent despite the fact that an untested choice of layer and foundational statutory term could have a negative impact on the overall utility and complexity of the adopted encryption exemption. Accordingly, in the case of state-based encryption exemptions, we would contend that the process of experimenting and layering has had a negative rather than positive effect.

6. Conclusion

The development of encryption safe harbors in US state-based data breach notification laws demonstrates the weaknesses of a non-uniformed approach. The plethora of definitions in operation needlessly complicates compliance for nationwide organizations. Some of these definitions are internally inconsistent and this appears to have been caused by the advent of a 'pick and mix' mentality. Some state legislatures have attempted to resolve concerns by developing more specific and developed definitions of encryption but these laws have also encountered problems due to the complexity of their definitions. Australia would do well to avoid these unnecessary problems and the ALRC's recommendations recognize the benefits to be gained from a uniformed approach to data breach notification that covers all states and organizations. We agree with this general approach which is particularly supported by our research into encryption safe harbors.

[103] *Id.*